Cloud computing and Privacy Issues – first reflections

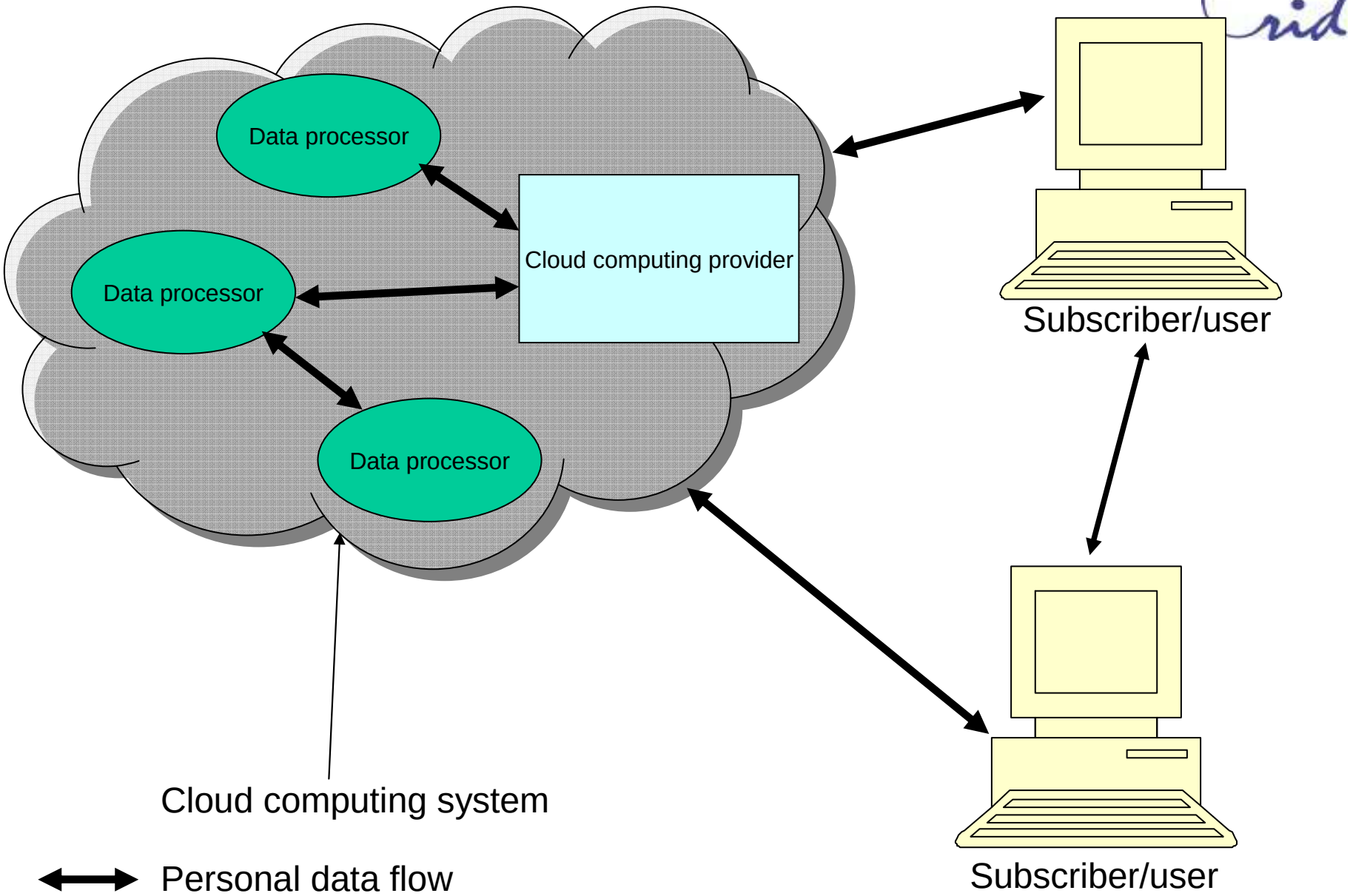
OCTOPUS Conference
Council of Europe
March, 25 2010

Y. POULLET et J.M. VAN GYSEGHEM
Faculty of Law - University of Namur
CRID
yves.poullet@fundp.ac.be
http://www.crid.be

Table of content

- Diversity of Cloud Computing Services (CLCS) and basic remarks
- How Cloud Computing is challenging the DP definitions?
- Duties of the actors…
- Security obligations?
- Liability of CLCS
- TBDF and Applicable law
- Conclusions

Introductory remarks



Introductory remarks

Diversity as regards CLCS models to be taken into account:

- As regards the **service** provided: from SaaS, Paas to IaaS…
- As regards the **openness** of the CLCS: Private, Community, Public and Hybrid clouds…
- As regards the **user/subscriber**: individuals/ Companies/Administration

Diversity of privacy issues related to the last classification

- Services to individuals (e.g. Social networks):
  - Right to be informed, consent, right to image, profiling, ownership and lot of data after the death.
  - Exception as regards domestic use.
- Services to companies:
  - business secret;
  - need to distinguish and define user, subscriber and data subject
  - specific regulation/prohibition as regards specific data (e.g. Health data)
- Services to public administrations: State's sovereignty

CLCS: A challenge as regards the DP definition

- Personal data: Do we need an extension of the Data protection to legal persons?

- Status of the actors:
  - QUESTIONS:
    - ***Can we consider CLCS provider as a data controller (controller of the file)?***
    - ***Can we consider that individuals/legal persons might be considered as data controller and CLCS provider as data processor?***
  - Source of reflexion:
    - ***As regards Directive 95/46, reference to « purposes** and **means ». Can we consider that « means »= to choose a CLCS offering appropriate security tools? What if CLCS is pursuing its own purposes or offering additional services? What's about data records by CLCS operator for achieving the security purposes?***
    - ***As regards Conv.108, no distinction between D.C. and D.P..***
    - ***Consequences of the qualification***
  - Both CLCS and individuals/legal persons are data controllers?

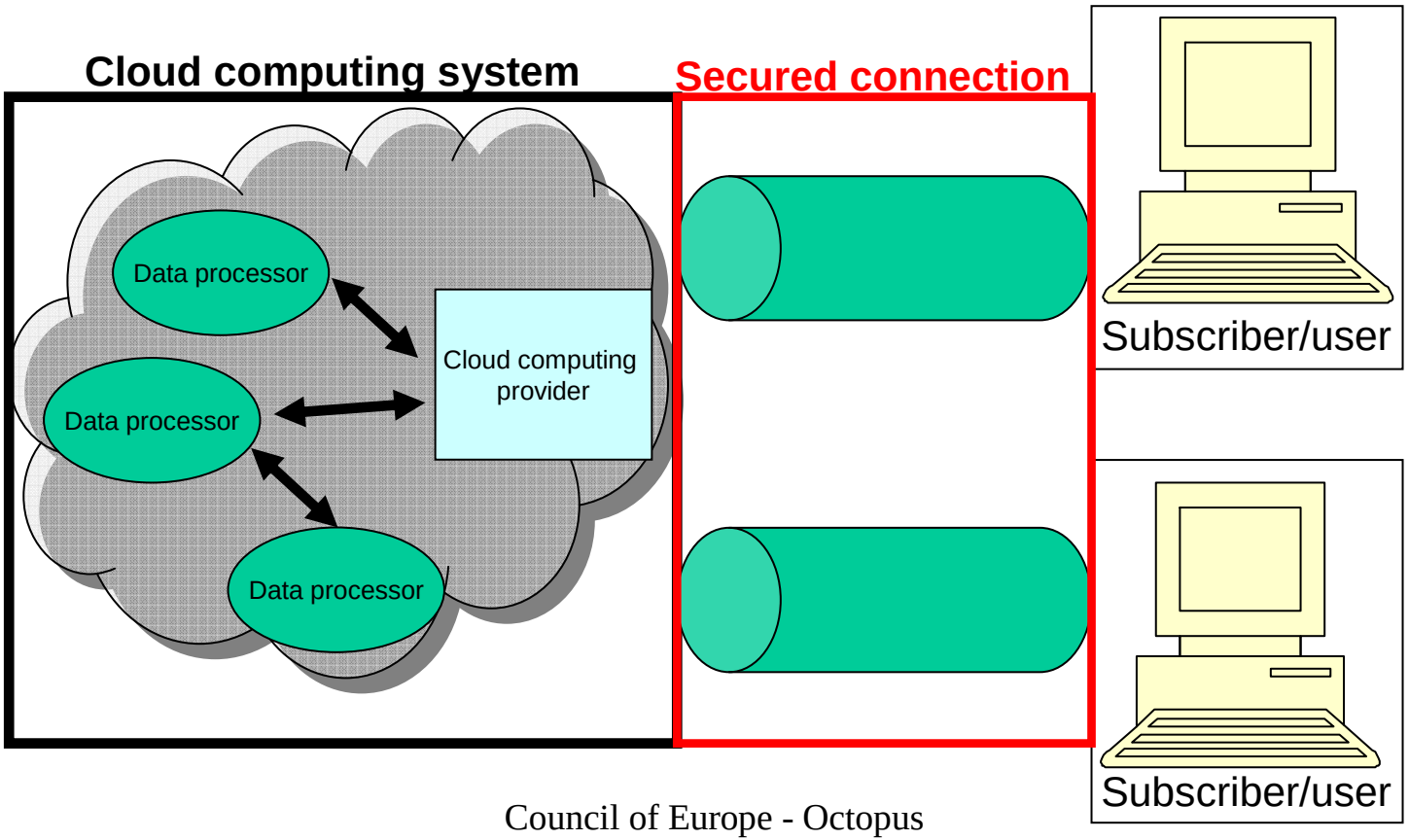
- Domestic use and Social network

CLCS: A challenge for data protection principles

- Principle of transparency and, beyond, which rights for the DS?
  - Obligation to inform about the recourse to a CLCS: do we need a specific information towards the subscriber (e.g. the Bank ot the hospital), the user (e.g. the Bank's employees or the physicians) and the other DS (e.g the Bank's customers or patients)?
  - Right to access: how to ensure the right to access when the data are at the CLCS data bases? Case of CLCS bankruptcy?
  - Can we speak about a ownership of the subscriber on his or her own data; obligation of the CLCS to erase the data in case of contract's cancellation?

CLCS: A challenge for data protection principles

- Principle of security
  - Security of transmission to the CLCS and security within the CLCS System



CLCS: A challenge for data protection principles

- Appropriate security measures to be supported by the subscriber?
  - ***What does mean the obligation for D.C. to use a D.P. of good quality (use of labelling system, need for ISO standards)?***
  - ***Is there any obligation to have specific clauses in case of termination of activities (problem of transfer and of bankruptcy)?***
  - ***Need to specify the main characteristics of the data processing (duration of the processing, categories of users, etc.) to be observed by the CLCS provider.***

CLCS: A challenge for data protection principles

- ***Appropriate security measures by the CLCS:***
  - ***Obligation to comply with the contractual requirements imposed by the subscriber.***
  - Information accountability principle (tell what you are doing and ensure that you will do what you are telling)
  - Standardisation as regards audit, nomination of a security obligation, data segregation,…
  - Obligations in case of security breach

Liability issues

- Each actor has its own liability:
  - Cloud computing provider (as data controller or data processor or even both):
    - Security;
    - Confidentiality;
    - Etc.
  - Subscriber/user (as data controller or data processor or even both):
    - Security of its own network;
    - Access precaution;
    - Etc.
  - Data processor of the Cloud computing provider:
    - Security;
    - Confidentiality;
    - Etc.

Liability issues

- Each duty leads to a liability;
- Need to be enforced by effective means?
  - By law?
  - By contract?
  - By selfregulatory initiatives?
  - By Standardization?
  - Etc.

TBD Flows and applicable law

- As regards data flows between C of E Member states, no restriction? Even for sensitive data?

- As regards data flows to third countries, the absolute need for CLCS to offer « adequate » protection (addtional protocol Conv. 108) through diverse means
  - Use of contractual models

  AND
  - Use of BCR (problem as regards the use of IS of other companies?)

  Q: What about the concept of adequacy as regards law enforcement authorities processing?

TBD Flows and applicable law

- As regards the applicable law?
  - If the subscriber/user is data controller and is established in the C of E territory and the CLCS is considered as data processor (outside of the C of E MS territories by working hypothesis), the C of E member states legislations are applicable
  - If the CLCS is considered as Data controller and is outside C of E territory, can we consider that CLCS is « using the equipment » of the subscriber (inside of the C of E MS territories by working hypothesis) to fall under the C of E Member states legislations?
    - ***If not, which criteria are the best to elect the applicable law?***
  - What's about the art.1 ECHR? « The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in S.1 of this Convention »
- Other issues:
  - Third Party Provision ?
  - Applicable law provision?
  - What's about a non transfer clause?
  - What's about the consent? Whose consent?

Conclusions

1) **Who are the actors of cloud computing? Do they need to be legally defined if it is not already the case? If they are already legally defined, do the definitions at stake need to be modified?**

   We identified five, sometimes overlapping, categories of actors: subscribers, users, data subjects, controllers (co-controllers) and data processors.

   Two principal questions:

   – Does the concept of data processor need to be defined under ETS 108?

   – Do legal persons need to be protected under the data protection rules of the ETS 108, as regards which data (extension of the definition of the personal data and, therefore, of the data subject)?

Conclusions

2) Which existing duties under ETS 108 need to be adapted? Which non-existing duties under ETS 108 need to be created? As the case may be, which actor has to bear these modifications or these creations?

More precisely:

- Should CLCS as data processors have to support specific duties provided for by the law, and which duties (e.g. in general as regards transparence and liability)?
- Should a specific duty as regards security breach have to be established? Who would have to support this new duty (provider and/or subscriber), towards which actor (subscriber and/or data subjects) and in which cases?
- How to treat the distinction between non-domestic and domestic processing activities? When is it still relevant and how to improve the protection of data subjects when a domestic use exception could apply (total exclusion of data protection law or establishment of a softer legal regime)?
- Should **data retention obligations** have to be imposed on cloud computing services providers, when and how?
- Due to the possible imbalance between the actors of the cloud, is **consent** always an adequate basis of the legitimacy of the processing at stake or should data controllers – and when – have a duty to found the legitimacy of their processing on an additional basis?

Conclusions

3) How what we could call the "data protection continuity" can be maintained?

This question can be subdivided into the following concerns:

- When the cloud computing service provider or its user (data subject) terminates the contractual relationship at stake, how can it be guaranteed that the data subject (user) will recover the total "ownership" (control) of data relating to him?
- In cases of bankruptcies, mergers of corporations or sales of corporations, etc, how can it be guaranteed that the level of protection originally ensured to the data subject will remain at least equivalent?

Conclusions

4) How to face the numerous concerns arising out of the international character inherent in cloud computing?

This wide question also needs to be sliced into parts:

- Do some specific cloud computing services (e.g. involving sensitive data) need to be forbidden when they imply transborder data flows between contracting States and, a fortiori, non-contracting States ensuring an adequate level of protection?
- Which concerns can be solved by corporate binding rules?
- How to assess the adequacy of non-contracting States to ETS 108 as regards the processing of personal data for **law enforcement purposes**?
- How far **consent and contract** could authorize transborder data flows outside the territories of contracting States, towards non-contracting States not ensuring an adequate level of protection?
- How to resolve conflict of laws concerns when, on the one hand, the actors involved in the cloud are located everywhere in the world and, on the other hand, a handy common conflict of laws rule does not exist yet between contracting States?
- Does the "territoriality" of data protection rules have to be differently defined depending on the duties (e.g. security or transparence) and the actors (data controller or data processor) at stake, and, as the case may be, how?

Thank you for your attention!